America's Health Insurance Plans

Statement for the Record

National Committee on Vital and Health Statistics

Subcommittee on Privacy, Confidentiality & Security

Prepared by:

Marilyn Zigmund Luke

Senior Counsel

202-861-1473

mzluke@ahip.org

America's Health Insurance Plans (AHIP) is the national association representing health insurance plans. Our members provide health and supplemental benefits to the American people through employer-sponsored coverage, the individual insurance market, and public programs such as Medicare and Medicaid. AHIP advocates for public policies that expand access to affordable health care coverage to all Americans through a competitive marketplace that fosters choice, quality, and innovation.

We appreciate the opportunity to share our perspectives related to the practical implementation of the Health Insurance Portability and Accountability Act's (HIPAA's) "minimum necessary" standard, to illustrate how health insurance plans approach implementation of that standard to ensure compliance, and our industry's commitment to HIPAA's standards. Our comments today represent our members' perspectives, specifically the Privacy Officers from a variety of health insurance plan types including national, mid-sized, regional, and local health insurance plans. **Overall, there was consensus among our members that HIPAA's minimum necessary requirements are working well and there is no need for significant regulatory changes.**

For example, health insurance plans currently have policies and procedures in place in a number of operational areas to ensure that the "minimum necessary" provision is effectively implemented in the day-to-day business operations.

- Privacy Officers often have implemented "checklists" to ensure that third-party requests for protected health information are properly verified and meet the minimum necessary rules before the information is sent to a third party (e.g., an attorney representing an individual in a personal injury civil suit).
- Covered entities utilize "role based access" policies to set parameters for staff members who need system and physical access to software, applications, or specific locations that contain protected health information in order to perform their day-to-day jobs.
- Security protocols establish which employees can access protected health information and when exceptions can/should be made. Scheduled, ongoing reviews of the protocols, such as desktop procedures, are performed.
- Some companies may have established oversight Committees that must meet before non-routine requests for disclosure of protected health information are granted, or to determine whether a more limited set of information can be disclosed to meet a request. This process ensures a thorough and objective review by experienced leaders within a company who understand the privacy and security requirements and can best assess such requests.
- Health insurance plans conduct corporate-wide training programs and departmental or targeted training for specific staff members when policies and procedures are developed and updated.

- Health insurance plan employees who are involved in key functions (e.g., claims processing) involving individuals' protected health information are trained to be highly-skilled and knowledgeable concerning the responsibility to maintain the privacy and confidentiality of data.
- Policies explain processes for employees to identify and report suspected privacy and/or security breaches, the facts and circumstances of which may implicate the minimum necessary requirement, in conjunction with other privacy and security rules.
- Most companies utilize internal audits or other assurance reviews to validate whether the policies and procedures are working as intended.

As the above examples illustrate, many of the policies and procedures address "minimum necessary" requirements, and also serve multiple compliance purposes by addressing other privacy and security requirements within the same policy and procedure. In addition, while we do not have specific statistics or research studies to share, the experience of our member companies demonstrates that consumers have not reported an inability to access their protected health information due to interpretations or related policies and procedures built on the minimum necessary provision. AHIP stands ready to address such challenges, working with other stakeholders and the U.S. Department of Health and Human Services, Office for Civil Rights (OCR), if the NCVHS hearings illustrate a need for improvements in this area.

Background on "Minimum Necessary"

When the HIPAA Privacy Rule was promulgated, the "minimum necessary" provision was considered a key component of the privacy infrastructure. Generally, the provision required covered entities to use, disclose, or request no more than the minimum necessary protected health information needed to accomplish the business function or task (e.g., coordinate an individual's care, process a claim for health care services).

As the Privacy Rule explained, some disclosures, such as sharing information with the individual are exempt from this requirement.[1] In addition, covered entities that utilize business associates are required to specify in written contracts the types of services the business associate will perform on behalf of the covered entity and the categories or types of protected health information the business associate will need to use and/or disclose in order to fulfill its services for the covered entity.

[1] E.g., disclosures made to: a health care provider for an individual's treatment; an individual's personal representative; HHS for complaint investigations or compliance reviews. Uses or disclosures: required by law; made pursuant to an individual's written authorization; or required for compliance with the HIPAA regulatory requirements.

The Privacy Rule recognized that it was the responsibility of the covered entity to develop and implement policies and procedures to reasonably limit uses and disclosures when the minimum necessary standard applies. For example, the covered entity's policies and procedures must identify the persons or classes of persons within the covered entity who need access to the information to carry out their job duties, the categories or types of protected health information needed, and conditions appropriate to such access.

We appreciate the guidance and the Frequently Asked Questions that OCR has issued to date on this topic.[2] That guidance explains, for example, that policies and procedures for routine or recurring requests and disclosures may be standard protocols that limit the protected health information disclosed or requested to the "minimum necessary" for that particular type of disclosure or request. Typically, review of such disclosures or requests is not required. Non-routine disclosures and requests, however, do require individual review to ensure compliance with the minimum necessary provision, along with other legal requirements under HIPAA and other laws, which use reasonable criteria for determining and limiting the disclosure or request to only the minimum amount of protected health information necessary to accomplish the purpose.

In certain circumstances, both the Privacy Rule and agency guidance recognize the concept of "reasonable reliance," meaning that a covered entity can rely on the judgment of the party requesting the disclosure that only the minimum amount of information being requested is what is needed from a "minimum necessary" standpoint, as illustrated by the following situations:

- A public official or agency states that the information requested is the minimum necessary for a purpose permitted by the Privacy Rule,[3] when the disclosure is required by law, for health oversight activities, for public health purposes, or other situations outlined in the regulations.
- Another covered entity is making the information request.
- A professional who is a workforce member or business associate of the covered entity holding the information states that the information requested is the minimum necessary for the stated purpose.
- A researcher has appropriate documentation from an Institutional Review Board or Privacy Board.

Ultimately, a covered entity retains discretion to make its own minimum necessary determination for disclosures to which the standard applies (i.e., the "reasonable reliance" concept permits, but does not compel, a covered entity to make any or all requested disclosures). This analytical process and the flexibility to evaluate specific

[2] *See generally,* http://www.hhs.gov/hipaa/index.html.
[3] 45 C.F.R. § 164.512.

situations are critical for good faith compliance, and avoidance of violations and significant penalties for violating the HIPAA privacy or security requirements.[4]

The Current Compliance Environment: "Minimum Necessary" Post HIPAA, HITECH Act, and Affordable Care Act (ACA) Implementation

Since the HIPAA statute and corresponding regulations were enacted, and the subsequent HITECH Act and corresponding regulations went into effect, we are aware that the "minimum necessary" requirements have been challenging for some organizations, as evidenced by the fact that compliance with this requirement is in the top five issues uncovered by OCR during the agency's complaint resolution and compliance investigations processes.[5] From the agency's publicly-available findings, it appears likely that many situations have occurred in which too much protected health information has been used and/or disclosed by a covered entity or a business associate.

One of the cornerstones of the minimum necessary provision is that a covered entity has flexibility in assessing what the minimum necessary parameters should be, based on the entity's business operations, for an information use or request for disclosure. We recognize that OCR makes settlement agreements available on the agency's website, and this transparency helps other entities understand the "lessons learned." Details remain unclear, however, about how entities failed to comply with the minimum necessary expectations. In addition, it would be helpful to understand whether individual consumers were affected, whether the non-compliance was based on administrative and/or human errors, and the types of corrective actions that were taken to satisfy OCR of an entity's or associate's commitment to compliance.

More information about violations or challenges that entities have experienced with implementing the minimum necessary provision would be helpful for consumers and across a multitude of organizations. For example, it would be helpful for OCR to describe the following:

- What specifically have covered entities done to be compliant with the minimum necessary provision? When was non-compliance evident?
- When OCR conducted a review, investigation, or audit, were written policies and procedures addressing minimum necessary parameters lacking, or were there more detailed steps that covered entities could have implemented to

[4] Additional details relating to the penalty structure and enforcement processes can be found on the Internet at: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.htm.

[5] Information available on the OCR website via the Internet at: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.

ensure compliance? If so, what were they and what did OCR recommend?

- What recommendations for modifying workflows or business processes, if any, were requested to come into compliance with the minimum necessary provision?
- In situations where violations were found, was too much, too little, or an incorrect type of protected health information used and/or disclosed by a covered entity or a business associate.
- Were minimum necessary compliance issues limited to a specific covered entity type, business associates, or were other factors involved in perceived areas of non-compliance?
- To the extent OCR can share the facts and circumstances related to minimum necessary and areas of improvement for covered entities and business associates, can these examples be shared with affected stakeholders without compromising the privacy and security of an individual or individuals?

As the questions help illustrate, all stakeholders can benefit from learning more about OCR's expectations for implementing the minimum necessary provision in a variety of business environments, including specific examples, facts, audit standards, and/or rationales used to support entities' compliance with ongoing minimum necessary refinements, when applicable.

Priority Areas for the Practical Application of HIPAA's Minimum Necessary Provision and Regulators' Oversight in the Current Health Care Community

HIPAA, the HITECH Act, and corresponding regulations, in conjunction with state laws and regulations that are more stringent than the HIPAA requirements, empower both federal regulators' oversight and state Attorneys' General enforcement of the privacy and security rules. This functionality has established a cohesive yet complicated oversight and enforcement framework for covered entities and their business associates, who work on a daily basis to ensure good faith compliance.

As noted above, we believe that overall the minimum necessary provisions are working well and no regulatory changes are necessary. We offer seven specific areas that we believe should be considered by the NCVHS Privacy, Confidentiality & Security Subcommittee before recommendations to the HHS Secretary are prepared. We respectfully request that the NCVHS encourage OCR to issue new or revised guidance on these topics, in addition to future public and private collaborations and hearings, when appropriate.

Appendix A, which is attached to this document, provides additional details and a cohesive rationale for our recommendations and conclusions, which include the following:

1. **Maintain the Flexibility that was built into the Minimum Necessary Provision.** The HIPAA rules need flexibility in order for covered entities to keep their business models functional and flexible to keep pace with new and emerging payment models, quality initiatives, and health care delivery systems.

2. **Address the Vulnerabilities of Secondary and "Downstream" Uses of Protected Health Information.** Consumers cannot benefit from privacy and security protections if non-HIPAA entities legitimately receive protected health information from a HIPAA covered entity or business associate, if the receiving non-HIPAA entity is not held to the stringent HIPAA/HITECH Act requirements and regulatory oversight mechanisms.

3. **Work to Align HIPAA and the Federal "Part 2" Confidentiality Regulations.** OCR should work with the HHS Substance Abuse and Mental Health Services Administration (SAMHSA) and key stakeholders to provide information about ways that HIPAA protects information about individuals' substance use disorders and treatments. OCR should work with SAMHSA, individual consumers, affected stakeholders, and Congress to leverage the HIPAA rules and align the corresponding federal Part 2 confidentiality requirements.

4. **Educate Individual Consumers About "Social Sharing."** Consumers utilize a variety of devices, online tools, and social media sites for health improvement, education, personal support, and other needs. By sharing information through these applications and sites, consumers may unintentionally negate the privacy and security protections of their health information. The Internet has great potential to positively impact patient care, but data security must be a top consideration. Consumers need to understand the risks and rely on common sense and competent service providers to ensure the proper handling of their health information.

5. **Explain Whether, When, or How the Minimum Necessary Provision May Apply in Cybersecurity Situations and Investigations.** All public and private entities have been and continue to be subject to cybersecurity attacks. OCR should work with federal agencies such as the Departments of Homeland Security and Justice, and consider issuing guidance for entities that face cybersecurity attacks, including HIPAA covered entities and their business associates.

6. **Provide a Status Update on the Electronic Claims Attachment Standard.** HIPAA covered entities that conduct electronic transactions should understand whether the electronic claims attachment standard will be adopted in the near future, and if so, how the "minimum necessary" provision can set parameters for requesting additional information from a health care provider without restricting the ability of an entity to request and receive information needed to process and adjudicate the electronic transaction.

7. **Expand Guidance on the "Firewalls" Between Group Health Plans and Employers.** Additional guidance would be helpful for employers to reinforce HIPAA's rules and the application of the minimum necessary requirement. OCR has issued Frequently Asked Questions (FAQs)[6] to explain how protected health information may be utilized for specific purposes. We believe that employers could benefit from more information that explains HIPAA's provisions.

Summary and Conclusion

We appreciate the opportunity to provide our perspectives on this important topic. We hope that our testimony helped to illustrate where additional clarification or real-life examples will further educate HIPAA covered entities and the consumers we serve so that individuals' health information will be protected, private, and secure, but also that individual patients, their family members and caregivers, treating health care providers, and other entities with a legitimate right to use and disclose protected health information can do so as allowed by the HIPAA Privacy Rule, the HITECH Act, state laws and regulations, and other applicable legal requirements.

[6] The FAQs are available on the Internet at the OCR website, http://www.hhs.gov/hipaa/index.html, and address situations where health information can be needed for workers' compensation, required by the Centers for Medicare and Medicaid Services (CMS) for retiree drug subsidies, and how privacy notices can be shared with individuals. *See,* 45 C.F.R. §164.504(f).

America's Health Insurance Plans

Statement for the Record

(June 16, 2016)

Appendix A

This Appendix provides a detailed discussion of key issues and recommendations noted in our Statement for the Record, which is offered in support of our public testimony before the National Committee on Vital and Health Statistics Subcommittee on Privacy, Confidentiality & Security in the

Maintain the Flexibility that was built into the Minimum Necessary Provision

The HIPAA rules need flexibility in order for covered entities to keep their business models functional and flexible to keep pace with new and emerging payment models, quality initiatives, and health care delivery systems. The ACA established new parameters and regulatory requirements for the health insurance community and their individual customers. New business models such as Accountable Care Organizations and other physician-owned health care systems started to emerge. Billing reforms including the new International Classification of Diseases, Tenth Revision (ICD-10) and the International Classification of Diseases, Tenth Revision, Clinical Modification (ICD-10 [CM]) were implemented. Corporate mergers and acquisitions took place or may be currently pending. New health insurance products were designed, the federally-facilitated and the state-based Exchanges were built and launched for the public's use, and changes to public programs such as Medicare and Medicaid have taken place. Health plans, including Medicare Advantage plans, have been designing and implementing innovative programs in areas such as care coordination and disease management to promote high value care. Also, proposed regulations were issued implementing the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA) that would change how Medicare incorporates quality measurement into physician payments and provide incentives for eligible practitioners participating in alternative payment models (APMs).[7] None of these developments were in existence at the time when the HIPAA and HITECH laws were enacted, the corresponding regulations were promulgated, or sub-regulatory guidance was issued.

The HIPAA rules need to keep pace with consumers' needs and expectations, the

[7] 81 Fed. Reg. 28161.

health care community's requirements, and changes that are taking place across the health care industry. **We fully support the flexibility that was built into the "minimum necessary" provision, and we encourage the Subcommittee to reinforce the need for organizations to retain such flexibility. Entities are in the best positions to understand and evaluate their business environments and changing operations to keep pace with developments sought by consumers, changes in the marketplace, and as designed and influenced by other federal and state legal requirements.**

Address the Vulnerabilities of Secondary and "Downstream" Uses of Protected Health Information

Several years ago, the NCVHS convened hearings to explore the concept of secondary uses of data. More recently, the Committee re-engaged stakeholders to assess whether the HIPAA de-identification parameters were sufficient or whether changes were needed to better protect the privacy, confidentiality, and security of individually-identifiable health information in a variety of settings and for use in different contexts (e.g., research). We commend the NCVHS for re-focusing its resources in this area. We believe that "big data" has become commonly used, and a variety of entities have become more sophisticated in programming algorithms or leveraging a variety of public and private data sources to glean information - whether to benefit the individual consumer, a private company's business interests, or perhaps a nefarious objective by a "bad actor" looking to commit medical identity theft or other criminal act.

Over time, our members and other HIPAA covered entities have been required to produce data in a variety of legitimate business contexts. Federal and state agencies often receive individually-identifiable health information for public health or oversight functions. Often, limited data sets are disclosed pursuant to a data use agreement between public and private entities.

Concerns have mounted as anecdotal examples and public discussions have focused on public or private entities' subsequent sharing of HIPAA-covered data with non-HIPAA covered individuals or organizations. The following examples are offered to illustrate these concepts:

- A state Exchange amasses large data sets relating to individuals from a variety of sources for legitimate reasons. A large portion of the data may be received from individual consumers and HIPAA-covered entities. If a state then utilizes a "data aggregator" to perform certain functions for the state-based Exchange, questions can arise relating to what function the data aggregator is performing, where the data is, and whether the "data aggregator" utilized other, unrelated data sets, and if so, for what purposes.

- Researchers may request public or private data sets to fulfill a specific research need. The researchers are often bound by written agreements that describe how the data can be used, disclosed, and disposed. Federal and state oversight of these arrangements can be limited, and private entities may be reluctant to participate in research projects without assurance that the third-party researchers will comply - and will be evaluated for compliance - with the contractual requirements.
- State all-payer claims databases (APCDs) may share or sell data to private entities. To date, it is unclear what the state APCDs have established to ensure that "once-HIPAA-covered health information" remains private and secure.

Individual consumers cannot benefit from HIPAA's privacy and security protections if non-HIPAA entities legitimately receive protected health information from a HIPAA covered entity or business associate, but then release it to a receiving person or entity without applying the stringent HIPAA/HITECH Act requirements and regulatory oversight mechanisms.

We encourage the NCVHS to advocate for more transparency from public entities that utilize HIPAA-covered data for their business functions. In addition, the Committee members should seek to evaluate the privacy and security parameters during tomorrow's state APCD hearings.

Work to Align HIPAA and the Federal "Part 2" Confidentiality Regulations

On April 11, 2016, AHIP submitted comments[8] in response to proposed regulations governing the confidentiality of substance use disorder patient records as published in the *Federal Register* on February 9, 2016.[9] Generally, we expressed support for SAMHSA's goal of modernizing the Part 2 regulations to facilitate care coordination and to increase the opportunities for individuals with substance use disorders to participate in new and emerging health care models. We indicated the need to protect the privacy of individuals' health information in alignment with current care delivery models and technological advances in how health information is accessed, used, disclosed, and protected.

In many situations, private entities have implemented special protections for substance use disorder and mental health information based on customer needs and in compliance with federal and state requirements. We believe additional efforts should focus on "modernizing" the Part 2 confidentiality rules to align with the HIPAA requirements, when possible.

[8] The letter is available at the federal regulatory portal, www.regulations.gov.

[9] 81 Fed. Reg. 6987.

Specifically, our letter recommended that SAMHSA should assess whether the existing relevant statutory requirements and agency authority are adequate to "modernize" the Part 2 regulatory requirements to keep pace with existing laws and regulations and industry developments while concurrently protecting the privacy and confidentiality of substance use disorder information. SAMHSA should then initiate the following actions:

- Necessary statutory changes should be noted and discussed in the preamble to the [SAMHSA] final rule so that Congress, SAMHSA, and other stakeholders can discuss changes to the statute that enable substance use disorder and other health information to be used and disclosed in ways that are aligned with and permitted by HIPAA;
- SAMHSA should encourage Congress to convene public hearings, through Advisory Committees such as the NCVHS, receive input from individuals, as well as public and private entities to evaluate proposals for statutory changes;
- SAMHSA should continue to review the Part 2 confidentiality regulations and/or delay issuing final regulations if currently pending legislative proposals are enacted that change the legal landscape for substance use disorder information and related protections; and
- SAMHSA, in conjunction with OCR, should issue updated guidance that explains how HIPAA currently protects substance use disorder information in addition to other types of health information. In addition, the guidance should explain how the HIPAA regulations allow health information to be used and disclosed for treatment, payment, and health care operations, and how the requirements applicable to substance use disorder information can align with HIPAA.

OCR should work with SAMHSA and key stakeholders to provide information about ways that HIPAA protects information about individuals' substance use disorders and treatments. OCR should also work with SAMHSA, individual consumers, affected stakeholders, and Congress to leverage the HIPAA rules and align the corresponding federal Part 2 confidentiality requirements.

Educate Individual Consumers About "Social Sharing"

Consumers utilize a variety of devices, online tools, and social media sites for health improvement, education, personal support, and other needs. By sharing information through these applications and sites, consumers may unintentionally negate the privacy and security protections of their health information.

Consumers are aware of website "Privacy Policies" or "Terms of Use" for the Internet sites they use. We believe that most consumers are unaware that sharing their own health information, or information about friends, relatives, or others, can be used by

some entities with data capabilities to compile and match non-public data sources to garner individual profiles or granular statistics about individuals, lifestyle choices, relatives, locations, interests, and a host of other personal data.

We support education campaigns or written materials to educate consumers about "social sharing" of their own and others' health information, and how doing so may have unintended consequences for information privacy and security.

Explain Whether, When, or How the HIPAA Minimum Necessary Provision May Apply in Cybersecurity Situations and Investigations

HIPAA covered entities, along with all public and private entities have been and continue to be subject to cybersecurity attacks. Cybersecurity is both an "old" and "new" area - meaning that for many years the U.S. Government, in conjunction with public and private entities, has been working to prepare for and defend against cyber attacks. Federal agencies such as the Departments of Homeland Security and Justice have been active and effective. In reality, the landscape continues to evolve as new techniques are used and new actors (e.g., foreign governments) are infiltrating private and secure electronic data of any type, whether the data relates to national security matters, corporate proprietary business secrets, individual health information, or other data sources.

A variety of agencies and entities have been and will continue to develop educational materials, detection plans, simulated tests mimicking cyber attacks, and other methods to help prevent, detect, and respond to cybersecurity events. AHIP is participating in several forums to engage with federal and state regulators and legislators, and to offer our support for such initiatives. The variety of cybersecurity activities in state and federal forums is appreciated.

HIPAA covered entities and their business associates are informed about the federal and state data breach requirements and each company is responsible for compliance. A cybersecurity attack may or may not result in a breach, and the facts and circumstances will control an entity's response and mitigation plans, including notification to appropriate agencies and/or officials.

Public and private entities could benefit from broader cybersecurity education, along with understanding more about coordination efforts, including when and which federal and/or state agencies can partner with and provide support or guidance to a private entity.

When evaluating the HIPAA minimum necessary requirements, consideration should be given to cybersecurity situations and whether, when, or how the

minimum necessary provision may apply in such situations and investigations, particularly if existing laws and regulations do not address what a covered entity or business associate should do when facing cyber attacks or related events.

Provide an Update on the Electronic Claims Attachment Standard

Earlier this year in mid-February, the NCVHS Standards Subcommittee held a public hearing to assess, among other things, the status of implementing the HIPAA requirements related to electronic standards for healthcare claims attachments. We have reviewed the NCVHS recommendation letter that was issued subsequent to the event.[10] In addition, we support the "minimum necessary" recommendations contained in the letter that was approved during yesterday's NCVHS meeting.[11] We appreciate the time and effort that the Committee and others have committed to understanding the needs and processes for claims attachment standards.

We do believe, however, that there is more work to be done. Unlike other HIPAA electronic transaction standards, the claims attachment protocols will be largely determined by the parties involved in the transaction, and the "minimum necessary" information will vary based on the facts and circumstances of an individual's medical situation. Health care providers, health insurance plans, standard-setting bodies, operating rule authors, and other stakeholders should convene to discuss and propose parameters for requesting additional information to support an electronic claim, without restricting the ability of an entity to request and receive information needed to process and adjudicate an electronic transaction.

In addition, we believe that HHS should clarify whether a claims attachment standard will be adopted in the near future, and if so, when and how the HIPAA "minimum necessary" provision will be determined by HHS and OCR from a compliance standpoint. OCR guidance will be essential for successful implementation of such a transaction since operating rules and business principles will apply in a variety of contexts and "minimum necessary" determinations will be made on a case-by-case basis.

---

[10] The letter is available on the NCVHS website via the Internet at: http://www.ncvhs.hhs.gov/wp-content/uploads/2013/12/2016-Ltr-to-Burwell-Findings-of-RC-Adm-Simp-June-2015-Hearing-Word.pdf.

[11] The letter is available on the NCVHS website via the Internet at: http://www.ncvhs.hhs.gov/wp-content/uploads/2016/04/Action-Item-NCVHS-Attachment-Letter_060316_NCVHScomm-002.pdf.

Expand Minimum Necessary Guidance on the "Firewalls" Between Group Health Plans and Employers

One final area that may benefit from future OCR guidance covers the differentiation between individuals who are responsible for administration of an employer-sponsored group health plan, as opposed to providing a function solely for the employer.

HIPAA has a long-established regulatory "firewall" between employers and the health insurers or health plans that provide employee benefits on a fully-insured or self-funded basis. Most employers appreciate the need to receive summary, non-identifiable information, as allowed by HIPAA, to protect the privacy and security of individuals' health. Some anecdotal scenarios suggest that additional guidance for group health plan sponsors may be needed, to ensure that protected health information is not utilized for purposes prohibited by HIPAA, but that also addresses some of the emerging developments in plan designs, as well as specific but limited situations where an individual's health information pertains to legitimate business functions for the individual's employment.[12]

[12] For example, questions have arisen for some employers that may need information necessary to allow an employee to enter the workplace and to determine an individual's compliance with public health requirements, such as the use and disclosure tuberculosis or other disease screenings.